Chapter 4: Authenticating and Accessing Domain Resources from Non-Domain Machines

In this chapter we describe the steps you need to take in order to access resources (disk shares, printers, etc.) on the FERMI domain if your machine is not a member of the domain, whether it is on-site or off-site.

4.1 Preparing to Authenticate

4.1.1 Step 1: Obtain FERMI Domain Account

You will need to obtain a Kerberos principal for the FERMI domain in order to access FERMI domain resources. See section 2.2 *Kerberos Principals and Primary Accounts*.

From your account, you'll be able to access domain resources across the network from your remote/home systems (with some restrictions as discussed below). You will be required to reset your Kerberos password for the FERMI domain as discussed in section 2.3 *Kerberos Passwords*.

4.1.2 Step 2: Verify Required TCP/IP Ports are Open

If your computer is connected to the Fermilab campus network, this step is not required.

There are two application layer protocols from which to choose; each of which uses different ports:

- NetBIOS is available for Windows 2000, Windows 9x, Windows ME, Windows NT, or Windows XP.
- The newer "NetBIOS-less" SMB (server message block) is available for Windows 2000 and Windows XP only, but is incompatible with use of the AFS client for Windows (the AFS client is discussed in section 6.2 *Windows AFS Client for File Transfers to AFS Space*).

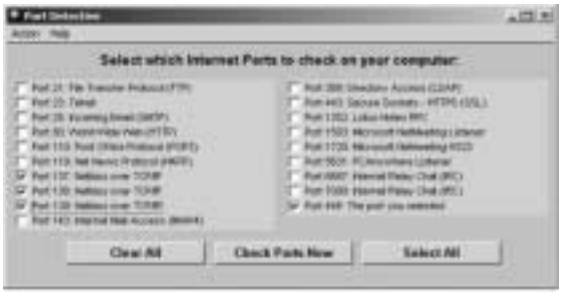
The required TCP/IP ports must be open when you connect to the Fermilab network. Fermilab blocks these ports except for certain servers. (To find out about particular servers, check with the server admin.) Even if a port for a

particular server isn't blocked by Fermilab, note that many ISPs block these ports. If your computer is not connected here at the lab, you'll need to use a tool to determine if these ports are open. Port Detective is a free tool available for download at `http://www.portdetective.com/`. The Computing Division does not guarantee the accuracy of this product. After you install this program, test for the required ports:

Protocol	OS	Port Numbers
NetBIOS	Windows 2K, NT, 9x, or ME, NT	137, 138 and 139
SMB[a]	Windows 2K or XP	445

a. Installation of the AFS client for Windows disables use of port 445 for SMB.

Here are a couple of sample screen shots from the Port Detective application, one for selecting ports...



and one that shows test results:

4.1.3 Step 3: Configure Machine to Use NTLMv2

The FERMI domain only accepts Kerberos or NTLMv2 (NT Lan Manager version 2) authentication. All Windows 2000 and XP systems that are members of the FERMI domain are configured to use Kerberos when the system is on-site. Computers that are not domain members must be configured to use NTLMv2. By default, non-domain Windows systems use the older NTLM (original version), which is not adequate. Read the Microsoft knowledgebase article Q239869 for the details on enabling NTLMv2 on your computer. Here we present a brief rundown on the steps needed to enable NTLMv2 for a variety of Windows operating systems.

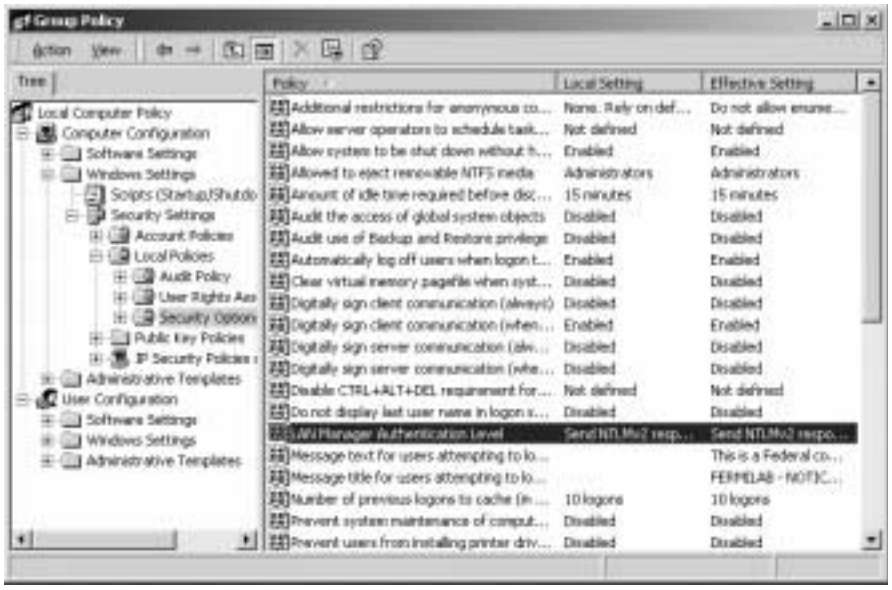
Windows 2000

W2K has NTLMv2 built-in, but you will have to activate it on your computer in order to perform NTLMv2 authentication. To do so, follow these steps:

1) Run gpedit.msc (Use **START > RUN...**, or **START > SETTINGS > CONTROL PANEL > ADMINISTRATIVE TOOLS > LOCAL SECURITY POLICY**).

2) In the left hand window, drill down to **COMPUTER CONFIGURATION/WINDOWS SETTINGS/SECURITY SETTINGS\LOCAL POLICIES\SECURITY OPTIONS**.

3) Select the key **LAN MANAGER AUTHENTICATION LEVEL**.



You will be presented with a dialog box similar to the following:

Choose **SEND NTLMV2 RESPONSE ONLY** or one of the variations to this option.

Windows XP

XP has NTLMv2 built-in, but you will have to activate it on your computer in order to perform NTLMv2 authentication. To do so, follow these steps:

1) Run gpedit.msc (use **START > RUN...**)

2) Drill down to **SECURITY SETTINGS\LOCAL POLICIES\SECURITY OPTIONS**

3) Select the key **NETWORK SECURITY: LAN MANAGER AUTHENTICATION LEVEL**.

Choose **SEND NTLMV2 RESPONSE ONLY** or one of the variations to this option.

Windows NT

If you have upgraded to Service Pack 6, then your desktop will support NTLMv2. You will have to enable NTLMv2 authentication. To do so, startup the registry editor (regedt32) and modify or add the key: **HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA\LMCOMPATABILITY LEVEL**. The level must be set to either 3 or 5 in order to enable NTLMv2; which you choose may depend on your prior setting.

Windows 98/Windows ME

Microsoft has an add-on for Windows 98 and ME that allow these operating systems to authenticate via NTLMv2. You can obtain a copy of the DSCLIENT software from the Windows 2000 CD-ROM under Clients\Win9x\Dsclient.exe. As is the case with NT4-based computers, registry entries will be required in order to activate NTLMv2 after installing the DSCLIENT software. We recommed that you read the entire Microsoft knowledgebase article Q239869 which discusses all of the necessary steps for enabling NTLMv2 on your computer.

Please note, the Computing Division does not support the Windows 98 or ME operating systems, and we do not make any guarantees that using the DSCLIENT will work.

4.2 Accessing Disk Shares

4.2.1 Using the Browse List

To access disk shares via **NETWORK NEIGHBORHOOD** or **MY NETWORK PLACES**, you must be on-site. Configure your TCP/IP settings to use Fermilab's Winservers. To do so, set your TCP/IP option for the WINS addressing to point to 131.225.9.31 and 131.225.110.15. WINS allows mapping between NetBIOS names and TCP/IP names.

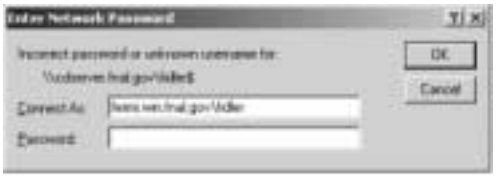
When you select a share you will be prompted for a network password. First enter your FERMI domain user account name (your Kerberos principal name) prefixed with `fermi\` to inform the system you are logging into the FERMI domain. E.g., enter `fermi\myname`. Then enter your Kerberos password for the FERMI domain. You should be able to access the share.

4.2.2 Mapping a Drive

If the TCP/IP ports are blocked, or you don't want to use the browse list (section 4.2.1), you can still map to disk shares using **MAP NETWORK DRIVE** if you know the specific share(s) you want to access.

For example, say you want to access share XYZ on testserver.fnal.gov. You can use the **MAP NETWORK DRIVE** (from the **MY COMPUTER** or **MY NETWORK PLACES** or from the Explore program) with the tools tab. Use the fully qualified server name if you do not have WINS defined, e.g., `\\testserver.fnal.gov\XYZ`.

Once you press the **FINISH** button, you will be prompted for a network password.

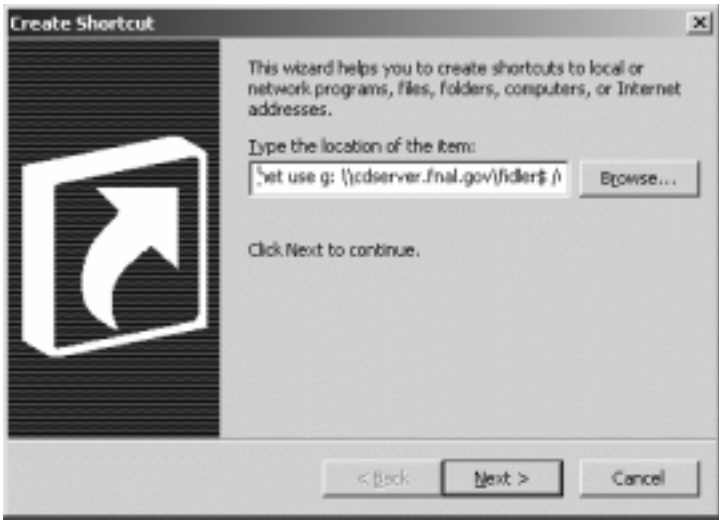


First enter your FERMI domain user account name (same as your Kerberos principal name) prefixed with `fermi.win.fnal.gov\` to inform the system you are logging into the FERMI domain. E.g., enter `fermi.win.fnal.gov\myname`. Then enter your Kerberos password for the FERMI domain. You should be able to access the share.

4.2.3 Setting up an ICON to do the Mapping

An easier way to set up common mappings of network disk shares is to use the command line program NET USE. You can create shortcuts for the file shares to which you frequently connect by creating shortcuts to the NET USE command.

For example, say you'd like an icon on your desktop that maps to your 'G' drive. Right-click on your desktop, and select **NEW > SHORTCUT** to create a shortcut that looks like this:



Note that in the example above the complete location in the field is:

```
Net use g: \\cdserver.fnal.gov\fidler$ /user:fidler@Fermi.win.fnal.gov
```

The format of the **`Net Use`** command under Windows 2000 is:

```
NET USE [devicename | *] [\\computername\sharename[\volume]
[password | *]]
        [/USER:[domainname\]username]
        [/USER:[dotted domain name\]username]
```

```
          [/USER:[username@dotted domain name]
          [[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {devicename | *} [password | *] /HOME

NET USE [/PERSISTENT:{YES | NO}]
```

4.3 Accessing Printers

4.3.1 From On-Site

Once you are authenticated, you can use any printer resource to which your account has access; the set of allowed resources varies by experiment or group. To authenticate, just map to any disk resource (section 4.2 *Accessing Disk Shares*).

4.3.2 From Off-Site

If your computer is not connected to the Fermilab campus network, you will not be able to print to any of the printers on-site. Fermilab imposes a block of the LPR ports at the border router. The same rules for browsing for a disk share resource (see section 4.2.1 *Using the Browse List*) apply to browsing for a printer resource.

4.4 Viewing the Active Directory

The Active Directory (AD) catalogs information about all the objects on a network, including people, computers, and printers, and distributes that information throughout your network. For all practical purposes, only computers in the FERMI domain will be able to view information in the AD. Native MicroSoft tools and AD browsing functions within **MY NETWORK PLACES** do not work unless your computer is a member of the FERMI domain.

4.5 Setting up Email

The recommended mail tool for offsite users is the IMAP server web interface. Simply point your web browser at the interface (the web page) corresponding to the server on which your email is stored (use `https` instead of `http`): `https://imapserver<n>.fnal.gov/`, where `<n>` is the server number 1, 2 or 3. This allows you access to your IMAP mail securely from anywhere with any web browser. For more information on the web email interface, see `http://computing.fnal.gov/email/`.

If you don't have an IMAP account or you would prefer not to use the web interface, you will need to use the SMTP gateway address of your Internet provider to send email to non-Fermilab addresses.